

Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G502 – Privacy Impact Assessments

CONTENTS:

- I. [Definitions](#)
- II. [Rationale](#)
- III. [Guideline](#)
- IV. [Procedure Reference](#)
- V. [Contact Information](#)
[Revision History](#)

I. DEFINITIONS

Chief Privacy Officer (CPO): A statewide function responsible for the development of policies, standards, guidance, and procedures related to the use, collection, maintenance and sharing of PII by State of Idaho agencies. The CPO provides agencies with training and guidance related to PII security controls and the completion of agency Privacy Impact Assessments (PIA) for PII embedded programs.

Personally Identifiable Information (PII) - Includes any of the following information related to a person:

1. Date of birth;
2. Social Security number;
3. Driver's license number;
4. Financial services account numbers, including checking and savings accounts;
5. Credit or debit card numbers;
6. Personal identification numbers (PIN);
7. Electronic identification codes;
8. Automated or electronic signatures;
9. Biometric data;
10. Passwords;
11. Parents' legal surname prior to marriage;
12. Home address or phone number;
13. Any other numbers or information that can be used to access a person's financial or health resources, obtain identification, act as identification, or obtain goods or services.

Identifying information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Privacy Impact Assessment: Is a structured process for identifying and mitigating privacy risks associated with the collecting, maintaining and disseminating information, ensures information handling conforms to applicable legal, regulatory, and policy requirements.

II. RATIONALE

It is the responsibility of all agencies within the State of Idaho to ensure compliance with legal, regulatory, and policy requirements related to the collection, use, maintenance of PII in support of mission and ongoing business operations. This guideline recommends best practices to support agency mission responsibilities while protecting the privacy of its citizens.

III. GUIDELINE

To reduce exposure of sensitive PII, agencies should minimize risk exposure by limiting the amount of personal information collected to only what is necessary to accomplish the agency's mission and limit the retention time of this information (in accordance with the State of Idaho's record retention requirements).

Agencies should conduct an internal inventory of all agency systems, storage media and data sources (e.g., databases, files, directories, etc.) that contain PII.

All agency information owners should conduct a Privacy Impact Assessment (PIA) to ensure compliance with legal, regulatory, and policy requirements, identify privacy risks and to identify methods to mitigate those risks associated with the collection, use, maintenance, and sharing of PII (NIST SP [800-122](#)).

PIAs represent a structured view of how the PII is used within the agency consisting of the following topics:

1. What authority does the agency have to collect PII;
2. What PII is being collected;
3. Why the PII is being collected;
4. The intended use of the PII;
5. With whom the PII will be shared;
6. How the PII will be secured (NIST SP [800-122](#));
7. Where the PII is stored.

Agencies should minimize the use, collection, maintenance, and sharing of PII by:

1. Only collecting for authorized business purposes;
2. Reviewing regularly to determine if collected PII is relevant;
3. Removing PII if it no longer serves a business purpose.

Agencies should develop procedures to:

1. Provide notice to individuals of the collection, use, maintenance, and dissemination of PII;
2. If not required by law, allow individuals to authorize agency collection of their PII;
3. Facilitate individual's access to review their PII for data quality and integrity;
4. Afford methods allowing individuals redress to correct inaccurate PII.

Agencies should utilize the [State of Idaho template](#) to document their PIA. Ideally, a PIA should be performed before:

1. Initialization of the governing system and when there is a material change to the system and/or underlying data requirements;
2. When making significant changes to an information system that creates new privacy risks for the information.

IV. PROCEDURE REFERENCE

NIST SP [800-122](#) (Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)).

ITA Enterprise Policy [P4560](#) (Data Breach Management).

V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

REVISION HISTORY

Effective Date: October 18, 2016